REMARKS

Claims 1-21 are presented for further examination. Claims 1, 9, 10, 13, 16, and 19 have been amended.

In the Office Action mailed August 19, 2009, the Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) as obvious over previously-cited Mills (U.S. Patent No. 6,311,204) in view of newly-cited U.S. Patent No. 7,165,180 ("Ducharme").

Applicants respectfully request reconsideration and further examination of the claims.

Claim Rejections

One of the counter-intuitive leaps made by the inventors of the present disclosure is the realization that a broadcast decryption and conditional access system can be constructed without the need for a smart card to maintain decryption data in secret. The Examiner has provided no reasoning as to why one of skill in the art would reject the conventional wisdom of the prior patents, which teach the use smart cards to distribute and safeguard secret data. The references cited and applied by the Examiner provide no teaching or suggestion to not use smart cards.

The claimed embodiments of the present disclosure provide a device on a monolithic circuit for decryption of broadcast signals that does not rely on a smart card to maintain the security of decryption keys used to decrypt the broadcast signals. As described in the present disclosure, prior systems that utilize smart cards are vulnerable to attack at the interface between the smart card and the decryption unit. One example of this is the Mills patent, relied upon by the Examiner, which relies on a smart card interface 80 for providing a secret key that is used to decrypt a service key received from a network interface module 12 via an interface 18. The service key is then used to descramble a control word related to an entitled program. The Ducharme reference, also relied upon by the Examiner in combination with Mills, describes a monolithic device that can store a key in a secure way, but it says nothing as to how the key store can be populated, much less whether multiple keys can be stored therein that are provided by broadcasts.

Turning to the claims, claim 1 is directed to a semiconductor integrated circuit that is provided as a monolithic circuit for decryption of broadcast signals. The monolithic circuit includes, *inter alia*, a processing unit (DVB 30) arranged to receive encrypted broadcast signals via an input interface (43) to decrypt encrypted broadcast signals in accordance with control signals (31) and to provide decrypted broadcast signals to an output interface on an output line (41).

The monolithic circuit also includes a first decryption circuit (32) arranged to receive encrypted control words that a decrypted into control signals in accordance with a decrypted common key from a dedicated common key store (36) in the integrated circuit. A second decryption circuit is also included and arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key (35) from a secret key store (34) in the integrated circuit and store the decrypted common key in the decrypted common key store (36).

Claim 1 also recites the circuit arranged such that the only route to placing a common key in the common key store (36) is to receive by broadcast the common key in encrypted form for decryption in accordance with the secret key (35) and the provide the common key to the common key store (36) over an internal bus (33). In addition, claim 1 recites that the only route to providing the control signals to the processing unit (38) is to input them in encrypted form for decryption in accordance with the decrypted common key.

As discussed in previous responses to office actions, which are incorporated herein, Mills does not teach or suggest a number of features recited in claim 1, including providing all of the circuit components on a monolithic circuit, storing a secret key on the monolithic circuit that is used to decrypt encrypted control words and to provide control signals to a processing unit that decrypts the broadcast signal. Mills also does not teach or suggest a dedicated common key store in the integrated circuit that then provides the decrypted common key to the processing unit.

In most of the embodiments of Ducharme, the store equated with the common key store (memory 130) is a read-only memory and, therefore, has no route to placing a common key in the store, at least during normal use. Ducharme does describe some embodiments where the

store 130 is a modifiable memory, such as a RAM. But in all embodiments featuring a RAM (see column 7, line 44 through column 8, line 21), the encryption key stored thereon is generated by the local encryption engine. Hence, Ducharme does not teach or suggest receiving an encryption key via broadcast in encrypted form or indeed encrypted at all.

There are some embodiments in Ducharme where the contents of a key register can be defined during the manufacturing processing by a third party. However, this is not by broadcast, and these accesses to select the content of the memory (130) are not via the encryption circuit (120). They are a direct access, which compromises security. Therefore, in Ducharme the keys are not provided in encrypted form for decryption prior to storage.

In addition, and most importantly, Ducharme does not teach or suggest storing of common keys, or any key, after decryption by the decryption unit (120). As mentioned above, in any embodiment that involves updating the memory portion (130), Ducharme teaches that the key is generated within the monolithic circuit without being encrypted.

Thus, applicants respectfully submit that the Examiner is incorrect when he asserts that the routing of common keys, as required by claim 1, is disclosed by Ducharme. Moreover, while the Examiner equates the storage portion (130) of Ducharme with the claimed common key store, it appears that Ducharme's storage portion (130) bears more resemblance to a private key store. (See col. 5, lines 37-62, and the embodiment described at col. 8, line 50 onward.)

Applicants further note that the Examiner seems to suggest at page 5, second paragraph of the Office Action, that neither Ducharme nor Mills discloses a secret key store located in the integrated circuit, or having a common key store and secret key store on the same monolithic device. The Examiner does not follow this up. Rather, he simply states that neither reference discloses this feature and that it would have been obvious to modify Mills in view of Ducharme to produce the current claimed embodiments. Applicants respectfully agree with the Examiner that the cited references do not disclose a secret key store on the same integrated circuit chip as the common key store. This is one of the inventive features of the present claimed embodiments.

In view of the foregoing, applicants respectfully submit that claim 1 is clearly allowable over the combination of Mills and Ducharme because neither reference, taken alone or in any combination thereof, teaches or suggests the claimed embodiment.

Dependent claims 2-7 are allowable for the features recited therein as well as for the reasons why claim 1 is allowable. For example, claim 7 recites the common key store arranged to store multiple common keys. This is not found in either Mills or Ducharme. Claim 5 recites the input interface having a separate input for the encrypted common key connected to the decryption circuit. Again, neither reference teaches this feature with respect to a common monolithic circuit.

Independent claim 9 is directed to a system for broadcasting signals to a plurality of subscribes that includes, *inter alia*, a transmitter and a plurality of receivers, each receiver having features similar to those described above with respect to claim 1. Likewise, claim 10 is directed to set top decoder device for decryption of broadcast signals that includes a monolithic device having a common key store, a secret key store, a decryption unit, a processing unit coupled to the decryption unit, and wherein the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and to provide the common key to the common key store over an internal bus, and with the only route to providing the control signals to the processing unit being to input them in encrypted form for decryption in accordance with the common key. As discussed above with respect to claim 1, neither Mills nor Ducharme teach or suggest these features. Applicants respectfully submit that claim 10, as well as dependent claims 11 and 12, are clearly allowable over the combination of Mills and Ducharme.

Independent claims 13 and 16 directed to methods of decrypting encrypted broadcast signals and for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, respectively. Both of these independent method claims include steps directed to decrypting encrypted common keys utilizing a stored secret key and to store the decrypted common in a common key store in the semiconductor integrated circuit. Control signals are decrypted with the common key to generate decrypted control signals that are used by a processing unit to decrypt the encrypted

broadcast signals. As with the prior independent claims, claims 13 and 16 recite features that are clearly distinguishable over the combination of Mills and Ducharme as discussed above with respect to claim 1. Hence, these claims and their respective dependent claims are allowable.

Independent claim 19 is directed to a system for broadcasting signals to a plurality of subscribers and to a plurality of receivers configured to receive the broadcast signals, each receiver comprising components similar to those recited in claim 1. Applicants respectfully submit that claim 19, as well as dependent claims 20 and 21, is allowable for the reasons discussed above with respect to claim 1.

In view of the foregoing, applicants respectfully submit that the claims in this application are clearly in condition for allowance. In the event the Examiner disagrees or finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jk

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1504288_1.DOC